Available online at www.sciencedirect.com

ScienceDirect

Journal of Number Theory 126 (2007) 185–192

JOURNAL OF Number Theory

www.elsevier.com/locate/jnt

Rational functions over finite fields having continued fraction expansions with linear partial quotients

Christian Friesen

Department of Mathematics, Ohio State University at Marion, Marion, OH 43302, USA

Received 9 March 2006; revised 19 June 2006

Available online 31 January 2007

Communicated by David Goss

Abstract

Let $\mathbb{F}$ be a finite field with q elements and let g be a polynomial in $\mathbb{F}[X]$ with positive degree less than or equal to $q/2$. We prove that there exists a polynomial $f \in \mathbb{F}[X]$, coprime to g and of degree less than g, such that all of the partial quotients in the continued fraction of g/f have degree 1. This result, bounding the size of the partial quotients, is related to a function field equivalent of Zaremba's conjecture and improves on a result of Blackburn [S.R. Blackburn, Orthogonal sequences of polynomials over arbitrary fields, J. Number Theory 6 (1998) 99–111]. If we further require g to be irreducible then we can loosen the degree restriction on g to $\deg(g) \leqslant q$.

MSC: 11J70; 11C08; 11K50

Keywords: Zaremba's conjecture; Finite fields; Continued fractions; Badly approximable polynomials

1. Introduction

A conjecture of Zaremba states that, for all positive integers $m \geqslant 2$ there exists an integer $1 \leqslant a < m$ such that all of the partial quotients in the continued fraction of a/m are less than or equal to 5. This has been proved for m being a power of 2, 3 and 5 by Niederreiter [3] and for m being a power of 6 by Yodphotong and Laohakosol [7]. The general case remains a conjecture.

We are interested in a version of Zaremba's conjecture that would apply to rational functions over finite fields. This has been investigated by Niederreiter [4], Mesirov and Sweet (in the char-

E-mail address: friesen.4@osu.edu.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2006.11.009

acteristic 2 case) [2] and more recently by Blackburn [1]. Let $\mathbb{F}$ be a finite field. Following the notation of Niederreiter [4] we define $K(f/g)$ to be the maximum degree of the partial quotients in the continued fraction of f/g where $f, g \in \mathbb{F}[X]$. We might be tempted to translate Zaremba's conjecture to the case of rational functions over finite fields by saying that, for all polynomials $g \in \mathbb{F}[X]$ with $\deg(g) \geqslant 1$ there must exist a polynomial $f \in \mathbb{F}[X]$, coprime to g, so that $K(f/g) \leqslant 5$ but a stronger conjecture may hold. Excluding only the case where $|\mathbb{F}| = 2$, Blackburn concludes his paper [1] by wondering if it could be true that for every polynomial $g \in \mathbb{F}$ there exists a polynomial f such that $K(f/g) = 1$. It should be noted, however, that Blackburn, who pursued his investigations with an eye to badly approximable functions, phrased his query using the language of orthogonal multiplicity. For our purposes, to say that g has positive orthogonal multiplicity is equivalent to saying that there is a polynomial f such that $K(f/g) = 1$ which means, as we shall see in Section 2, that there is a polynomial f such that $K(g/f) = 1$.

One of the two major results of Blackburn's paper [1] is the following theorem: Let d be a positive integer. Let $\mathbb{F}$ be a field such that $|\mathbb{F}| \geqslant \frac{1}{2}d(d+1)$. Then every monic polynomial $f \in \mathbb{F}[X]$ of degree d has positive orthogonal multiplicity.

We shall improve upon the bound above (effectively replacing $\frac{1}{2}d(d+1)$ by $2d$) in the following result:

Theorem 1. *Let $\mathbb{F}$ be a finite field. Let $g \in \mathbb{F}[X]$. If $0 < \deg(g) \leqslant \frac{1}{2}|F|$ then there is a polynomial $f \in \mathbb{F}[X]$, coprime to g and of degree less than g, such that all the partial quotients of the continued fraction of g/f have degree* 1.

If we restrict our attention to those polynomials g that are irreducible then we can loosen the restriction on the size of the polynomial by a factor of 2.

Theorem 2. *Let $\mathbb{F}$ be a finite field. Let $g \in \mathbb{F}[X]$ be an irreducible polynomial. If $0 < \deg(g) \leqslant |F|$ then there is a polynomial $f \in \mathbb{F}[X]$, coprime to g and of degree less than g, such that all the partial quotients of the continued fraction of g/f have degree* 1.

2. Preliminaries

Readers interested in an overview of basic results concerning continued fractions are referred to works of Perron [5] and van der Poorten [6]. We will recreate, in the context of our function fields, only a few facts which we shall need later on. Fix $\mathbb{F}$ to be a finite field with q elements and let X be an indeterminate. Let $A_0, A_1, \ldots, A_k \in \mathbb{F}[X]$ be polynomials of positive degree, with the possible exception of A_0. We write $[A_0, A_1, \ldots, A_k]$ as shorthand for the continued fraction $A_0 + 1/(A_1 + 1/(A_2 + \cdots + 1/A_k))$.

If $P, Q \in \mathbb{F}[X]$ are polynomials with $\gcd(P, Q) = 1$ and $\deg(Q) \geqslant 1$ then P/Q has a unique continued fraction $[A_0, A_1, \ldots, A_k]$ with $A_0, A_1, \ldots, A_k \in \mathbb{F}[X]$ and $\deg(A_i) \geqslant 1$ for $1 \leqslant i \leqslant k$. The partial quotients, A_i, can be determined by iteratively applying the division algorithm.

Definition 1. Define P_i and Q_i by $P_{-1} = 1$, $P_0 = A_0$ and $P_{i+1} = A_{i+1}P_i + P_{i-1}$ and $Q_{-1} = 0$, $Q_0 = 1$ and $Q_{i+1} = A_{i+1}Q_i + Q_{i-1}$. Then $P_i/Q_i = [A_0, A_1, \ldots, A_k]$ where the right-hand side of the equation is the unique continued fraction expansion of P_k/Q_k.

In matrix notation we can write

$$\begin{pmatrix} P_k & Q_k \\ P_{k-1} & Q_{k-1} \end{pmatrix} = \begin{pmatrix} A_k & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} A_{k-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} A_{k-2} & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} A_0 & 1 \\ 1 & 0 \end{pmatrix}$$

and transposing the matrix results in

$$\begin{pmatrix} P_k & P_{k-1} \\ Q_k & Q_{k-1} \end{pmatrix} = \begin{pmatrix} A_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} A_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} A_{k-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} A_k & 1 \\ 1 & 0 \end{pmatrix}.$$

Examining the determinants in the above expression shows that $P_{k-1}Q_k - P_kQ_{k-1} = (-1)^k$.

Lemma 1. *If* $\gcd(P, Q) = 1 = \gcd(R, S)$ *with* $\deg(P) > \deg(Q)$ *and* $\deg(R) > \deg(S)$ *and if* $P/Q = [A_0, A_1, \ldots, A_n]$ *and* $R/S = [B_0, B_1, \ldots, B_k]$ *then there is a polynomial* $V \in \mathbb{F}[X]$ *such that* $[A_n, \ldots, A_1, A_0, B_0, B_1, \ldots, B_k] = U/V$ *where* $\gcd(U, V) = 1$ *and* $U = PQ + RS$.

Proof. Let $U/V = [A_n, \ldots, A_1, A_0, B_0, B_1, \ldots, B_k]$. Then

$$\begin{aligned} \begin{pmatrix} U & ? \\ V & ? \end{pmatrix} &= \begin{pmatrix} A_n & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} A_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} B_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} B_k & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} P & Q \\ ? & ? \end{pmatrix} \begin{pmatrix} R & ? \\ S & ? \end{pmatrix} = \begin{pmatrix} PR + QS & ? \\ ? & ? \end{pmatrix} \end{aligned}$$

where we use ? to represent quantities of no immediate interest to us. Since the discriminant of the above matrix is ± 1 it follows that $\gcd(U, V) = 1$. Note that the hypotheses $\deg(P) > \deg(Q)$ and $\deg(R) > \deg(S)$ serve to ensure that A_0 and B_0 were non-zero and therefore that our resulting continued fraction has proper form. This concludes the proof. □

Definition 2. For $P, Q \in \mathbb{F}[X]$ with $\gcd(P, Q) = 1$ and $\frac{P}{Q} = [A_0, A_1, \ldots, A_k]$, define $K(P/Q)$ as $\max(\deg(A_i))$, $0 \leqslant i \leqslant k$.

Let $f/g = [A_0, A_1, A_2, \ldots, A_k]$. The reciprocal has a related continued fraction, namely:

$$\begin{aligned} g/f &= [0, A_0, A_1, A_2, \ldots, A_k] \quad \text{if } A_0 \neq 0, \\ g/f &= [A_1, A_2, \ldots, A_k] \quad \text{if } A_0 = 0. \end{aligned}$$

From the above it is clear that $K(f/g) = K(g/f)$.

Lemma 2. *Let* $\mathbb{F}$ *be a finite field. Define* $q = |\mathbb{F}|$ *and let* k *be a positive integer. The number of fractions of the form* g/f *with* $\deg(f) < \deg(g) = k$ *and* $\gcd(f, g) = 1$ *is* $(q-1)q^{2k-1}$.

Proof. The total number of ways of breaking k into an ordered sum of n positive integers is given by the binomial coefficient $\binom{k-1}{n-1}$ and there are exactly $(q-1)q^d$ polynomials of degree d. It follows that there are $\binom{k-1}{n-1}(q-1)^n q^k$ ordered sets of positive degree polynomials $\{A_0, A_1, \ldots, A_{n-1}\}$ such that $\sum_{i=0}^{n-1} \deg(A_i) = k$. Each such set defines, through the continued

fraction $[A_0, A_1, \ldots, A_{n-1}] = g/f$, a unique pair of polynomials f and g satisfying the above conditions. We finish the proof by summing over all possible values of n:

$$\sum_{n=1}^{k} \binom{k-1}{n-1} (q-1)^n q^k = (q-1)q^k \sum_{n=1}^{k} \binom{k-1}{n-1} (q-1)^{n-1} = (q-1)q^{2k-1}. \qquad \square$$

Lemma 3. *Let $\mathbb{F}$ be a finite field and k a non-negative integer. Define $q = |\mathbb{F}|$ and choose positive-degree polynomials $A_0, A_1, \ldots, A_k \in \mathbb{F}[X]$. Define $d = \sum_{i=0}^{k} \deg A_i$. Select $g \in \mathbb{F}[X]$ with $\deg(g) = n \geqslant 2d$. Then there are exactly q^{n-2d} polynomials $f \in \mathbb{F}[X]$ with $\deg(f) < \deg(g)$ such that g/f has a continued fraction expansion that begins with $[A_0, A_1, \ldots, A_k, \ldots]$.*

It is important to note that the f that we obtain here need not be coprime to g.

Proof. Let α, β be the coprime polynomials defined by $\alpha/\beta = [A_k, A_{k-1}, \ldots, A_1, A_0]$. It is clear that $\deg(\alpha) = \sum_{i=0}^{k} \deg(A_i) = d$. Consider the solutions (μ, ρ) to the equation $g = \alpha\mu + \beta\rho$. Since $\gcd(\alpha, \beta) = 1$ there must exist solutions to this equation and all solutions are given by the parametrization $(\mu, \rho) = (\mu_0 + T\beta, \rho_0 - T\alpha)$ for $T \in \mathbb{F}[X]$ where (μ_0, ρ_0) is any given solution. We may choose (μ_0, ρ_0) with ρ_0 of minimal degree, satisfying $\deg(\rho_0) < \deg(\alpha) = d$. Since $\deg(\beta) = \sum_{i=0}^{k-1} \deg(A_i) = \deg(\alpha) - \deg(A_k) < d$ it follows that $\deg(\beta\rho_0) < d + d \leqslant \deg(g)$. From this we see that $\deg(g) = \deg(\alpha\mu_0 + \beta\rho_0) = \deg(\alpha\mu_0) = d + \deg(\mu_0)$ and therefore $\deg(\mu_0) = n - d$.

Let $D = \gcd(\mu, \rho)$ and write $\mu = D\tilde{\mu}$ and $\rho = D\tilde{\rho}$ where $\gcd(\tilde{\mu}, \tilde{\rho}) = 1$. Then every choice of polynomial T leads to a unique combination of D and a continued fraction $\tilde{\mu}/\tilde{\rho} = [B_0, B_1, \ldots, B_j]$.

It will be necessary to ensure that $\deg(B_0) > 0$ before applying Lemma 1. This is equivalent to the condition that $\deg(\mu) > \deg(\rho)$. If $T = 0$ then $\deg(\rho) = \deg(\rho_0) < d \leqslant n - d = \deg(\mu_0) = \deg(\mu)$ and we are done. If $T \neq 0$ then, having chosen ρ_0 of minimal degree, we see that $\deg(\rho) = \deg(\rho_0 - T\alpha) = \deg(T\alpha) = \deg(T) + d$. Since $\deg(\alpha) > \deg(\beta)$ and since we wish to have $\deg(\mu) > \deg(\rho)$ it follows from $n = \deg(g) = \deg(\alpha\mu + \beta\rho)$ that we need $\deg(\mu) = n - d > \deg(\rho)$. Thus the condition $\deg(\mu) > \deg(\rho)$ is equivalent to the requirement that $\deg(T) < n - 2d$, which is true of exactly q^{n-2d} choices of polynomial T.

We conclude that there are q^{n-2d} pairs of polynomials $(\mu, \rho) = (D\tilde{\mu}, D\tilde{\rho})$ such that $g/D = \tilde{g} = \alpha\tilde{\mu} + \beta\tilde{\rho}$ and where $\tilde{\mu}/\tilde{\rho} = [B_0, B_1, \ldots, B_j]$ for some positive integer j and some positive-degree polynomials $B_0, B_1, \ldots, B_j$. It follows from Lemma 1 that $[A_0, A_1, \ldots, A_k, B_0, B_1, \ldots, B_j] = \tilde{g}/\tilde{f}$ for some polynomial $\tilde{f}$ coprime to $\tilde{g}$ and satisfying $\deg(\tilde{f}) < \deg(\tilde{g})$. Let $f = D\tilde{f}$ to see that $g/f = [A_0, A_1, \ldots, A_k, B_0, B_1, \ldots, B_j]$ as required. $\square$

Corollary 3. *Let $\mathbb{F}$ be a finite field and k a non-negative integer. Define $q = |\mathbb{F}|$ and choose positive-degree polynomials $A_0, A_1, \ldots, A_k \in \mathbb{F}[X]$. Define $d = \sum_{i=0}^{k} \deg A_i$. Select $g \in \mathbb{F}[X]$ with $\deg(g) = n \geqslant 2d$. Then there are exactly q^{n-2d} polynomials $f \in \mathbb{F}[X]$ with $\deg(f) < \deg(g)$ such that g/f has a continued fraction expansion that ends with $[\ldots, A_0, A_1, \ldots, A_k]$.*

Before beginning with the proof, we remark that, as was the case in the previous lemma, the polynomials f that are obtained here are not necessarily coprime to g.

Proof. From the lemma above we know that there are q^{n-2d} polynomials $f \in \mathbb{F}[X]$ with $\deg(f) < \deg(g)$ such that g/f has a continued fraction expansion that begins with $[A_k, \ldots,$

$A_1, A_0, \ldots]$. For any such polynomial f, let $D = \gcd(f, g)$ and write $\tilde{f} = f/D$ and $\tilde{g} = g/D$. Then $g/f = \tilde{g}/\tilde{f} = [A_k, \ldots, A_1, A_0, B_0, B_1, \ldots, B_j]$ and

$$\begin{pmatrix} A_k & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} A_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} A_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} B_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} B_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} B_j & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \tilde{g} & \tilde{x} \\ \tilde{f} & \tilde{y} \end{pmatrix}$$

for some polynomials $\tilde{x}$ and $\tilde{y}$. Taking the transpose gives

$$\begin{pmatrix} \tilde{g} & \tilde{f} \\ \tilde{x} & \tilde{y} \end{pmatrix} = \begin{pmatrix} B_j & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} B_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} B_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} A_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} A_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} A_k & 1 \\ 1 & 0 \end{pmatrix}.$$

Since all of the partial quotients have positive degree we see that $\deg(\tilde{x}) < \deg(\tilde{g})$. Letting $x = D\tilde{x}$ gives $g/x = \tilde{g}/\tilde{x} = [B_j, \ldots, B_0, A_0, A_1, \ldots, A_k]$. This demonstrates that there is a 1-1 correspondence between the set of polynomials f such that the continued fraction of g/f begins with a specified set of partial quotients and the set of polynomials x such that the continued fraction of g/x ends with those specified partial quotients in reverse order. Our desired conclusion follows. □

Definition 3. Let $g \in \mathbb{F}[X]$ have positive degree. Define $\Phi(g)$ as the number of polynomials f such that $\deg f < \deg g$ and $\gcd(f, g) = 1$.

Note: If P is an irreducible polynomial of positive degree d then there are $q^d - 1$ polynomials of lesser degree that are coprime to P, so $\Phi(P) = q^d - 1$. It is also clear that $\Phi(P^n) = (q^d - 1)q^{(n-1)d}$ for P irreducible. Since Φ is a multiplicative function and $(q^d - 1)q^{(n-1)d} \geqslant (q-1)^{nd}$ we obtain the inequality $\Phi(g) \geqslant (q-1)^{\deg(g)}$ which we shall make use of in the next section.

3. Proofs of the main results

We are now prepared to prove the two main theorems of this paper. The key idea is to show that there must exist a polynomial, f, coprime to g, such that the continued fraction for g/f has both the front half (the first k partial quotients) and the back half (the last k partial quotients) made up only of linear polynomials.

Theorem 1. *Let $\mathbb{F}$ be a finite field. Let $g \in \mathbb{F}[X]$. If $0 < \deg(g) \leqslant \frac{1}{2}|F|$ then there is a polynomial $f \in \mathbb{F}[X]$, coprime to g and of degree less than g, such that all the partial quotients of the continued fraction of g/f have degree* 1.

Proof. Let $q = |\mathbb{F}|$. We begin with the case where g has even degree: $\deg(g) = 2k \leqslant q/2$. Consider any of the $(q-1)^k q^k$ k-tuples of linear polynomials $(A_0, A_1, \ldots, A_{k-1})$. By Lemma 3, each such k-tuple is the first part of the continued fraction expansion of g/f for exactly one polynomial f of degree less than g. It follows that there are $q^{2k} - (q-1)^k q^k = q^k(q^k - (q-1)^k)$ polynomials f, of degree less than $2k$, such that the continued fraction of g/f does not begin with at least k linear partial quotients. Using Corollary 4 we similarly note that there are $q^k(q^k - (q-1)^k)$ polynomials f, of degree less than $2k$, such that the continued fraction of g/f does not end with at least k linear partial quotients. There are also $q^{2k} - \Phi(g)$ polynomials f, of degree less than $2k$, that are not coprime to g. Removing these three sets from the set of all

polynomials f of degree less than $2k$ gives us at least $q^{2k} - 2q^k(q^k - (q-1)^k) - (q^{2k} - \Phi(g))$ polynomials f of the kind required by the theorem. That quantity is positive if we have

$$2q^k\big(q^k - (q-1)^k\big) < \Phi(g). \tag{1}$$

Since

$$\Phi(g) = q^{\deg(g)} \prod_{\text{prime } p|g} \left(1 - \frac{1}{q^{\deg(p)}}\right) \geqslant (q-1)^{2k},$$

it will suffice to show that $2q^k(q^k - (q-1)^k) < (q-1)^{2k}$. We may rewrite the desired inequality as $(1 - \frac{1}{q})^{2k} + 2(1 - \frac{1}{q})^k - 2 > 0$. We verify that

$$\left(1 - \frac{1}{q}\right)^{2k} + 2\left(1 - \frac{1}{q}\right)^k - 2 > 1 - \frac{2k}{q} + 2 - \frac{2k}{q} - 2 = 1 - \frac{4k}{q} \geqslant 0$$

since $\deg(g) \leqslant \frac{1}{2}|\mathbb{F}|$ implies that $k \leqslant q/4$.

We continue our proof with the case where g has odd degree. Let $\deg(g) = 2k+1 \leqslant q/2$. Consider any of the $(q-1)^k q^k$ k-tuples of linear polynomials $(A_0, A_1, \ldots, A_{k-1})$. By Lemma 3, each such k-tuple is the first part of the continued fraction expansion of g/f for exactly q polynomials f with $\deg(f) < 2k+1$. It follows that there are $q^{2k+1} - (q-1)^k q^{k+1} = q^{k+1}(q^k - q(q-1)^k)$ polynomials f, of degree less than $2k+1$, such that the continued fraction of g/f does not begin with at least k linear partial quotients. Using Corollary 4 we similarly note that there are $q^{k+1}(q^k - (q-1)^k)$ polynomials f, of degree less than $2k$, such that the continued fraction of g/f does not end with at least k linear partial quotients. Note that if the first k terms in the continued fraction g/f are linear and if the last k are linear then there must be one more partial quotient in the middle that must be linear since $\sum_i \deg(A_i) = \deg(g)$. There are also $q^{2k+1} - \Phi(g)$ polynomials f, of degree less than $2k+1$, that are not coprime to g. Removing the three sets above from the set of all polynomials f of degree less than $2k+1$ gives us at least $q^{2k+1} - 2q^{k+1}(q^k - (q-1)^k) - (q^{2k+1} - \Phi(g))$ polynomials f of the required kind. That quantity is positive if and only if we have

$$2q^{k+1}\big(q^k - (q-1)^k\big) < \Phi(g). \tag{2}$$

Since $\Phi(g) \geqslant (q-1)^{2k+1}$ it would be enough to show that $(q-1)^{2k+1} - 2q^{k+1}(q^k - (q-1)^k) \geqslant 0$. We rewrite the desired inequality as $(1 - \frac{1}{q})^{2k+1} + 2(1 - \frac{1}{q})^k - 2 > 0$ and verify that

$$\left(1 - \frac{1}{q}\right)^{2k+1} + 2\left(1 - \frac{1}{q}\right)^k - 2 > 1 - \frac{2k+1}{q} + 2 - \frac{2k}{q} - 2 = 1 - \frac{4k+1}{q} > 0$$

because of our hypothesis that $2k+1 \leqslant q/2$. □

In the language of orthogonal sequences of polynomials, such as was used by Blackburn [1], our theorem becomes

Theorem 4. *Let d be a positive integer. Let $\mathbb{F}$ be a field such that $|\mathbb{F}| \geqslant 2d$. Then every polynomial $f \in \mathbb{F}[X]$ of degree d has positive orthogonal multiplicity.*

It is possible for us to cut the lower bound, on the size of the polynomials g, in half if we restrict ourselves to irreducible polynomials g. We shall conclude the paper by proving, as promised in the introduction, the theorem below.

Theorem 2. *Let $\mathbb{F}$ be a finite field. Let $g \in \mathbb{F}[X]$ be an irreducible polynomial. If $0 < \deg(g) \leqslant |F|$ then there is a polynomial $f \in \mathbb{F}[X]$, coprime to g and of degree less than g, such that all the partial quotients of the continued fraction of g/f have degree* 1.

Proof. Let $|\mathbb{F}| = q$. The theorem is trivially true when $\deg(g) = 1$ as one may choose $f = 1$. We next isolate the special case where $q = 2$ and $\deg(g) = 2$. There is only irreducible polynomial of degree 2 that is possible, namely $g = X^2 + X + 1$. Choosing $f = X$ gives us $g/f = [X + 1, X]$ and we have shown the theorem holds for this case.

If $\deg(g) = 2k$ then we follow through with the proof of Theorem 1 until we arrive at Eq. (1) where we replace $\Phi(g)$ with its value, $q^{2k} - 1$ and divide both sides by $2q^{2k}$ to get the inequality we wish to verify, namely

$$\left(1 - \frac{1}{q}\right)^k > \frac{1}{2} + \frac{1}{2q^{2k}}. \tag{3}$$

Looking to the case where $\deg(g) = 2k + 1$ and $\Phi(g) = q^{2k+1} - 1$ we use Eq. (2) to arrive at the following inequality which we need to prove:

$$\left(1 - \frac{1}{q}\right)^k > \frac{1}{2} + \frac{1}{2q^{2k+1}}. \tag{4}$$

Since Eq. (3) will imply Eq. (4) we only need prove the former. If $k = 1$ and $q \geqslant 3$ then Eq. (3) obviously holds, as it does also when $k = 2$ and $q \geqslant 4$. We now treat $k \geqslant 3$ and $q \geqslant 6$. Recall that $k \leqslant q/2$. Then we finish by expanding the left-hand side out to the first four terms to see that

$$\begin{aligned}\left(1 - \frac{1}{q}\right)^k \geqslant \left(1 - \frac{1}{2k}\right)^k &\geqslant 1 - \frac{k}{2k} + \frac{k(k-1)}{8k^2} - \frac{k(k-1)(k-2)}{48k^3} \\ &= \frac{1}{2} + \frac{5}{48} - \frac{1}{16k} - \frac{1}{48k^2} \\ &> \frac{1}{2} + \frac{1}{2 \cdot 6^6} > \frac{1}{2} + \frac{1}{2q^{2k}}\end{aligned}$$

since $k \geqslant 3$. □

References

[1] S.R. Blackburn, Orthogonal sequences of polynomials over arbitrary fields, J. Number Theory 68 (1998) 99–111.
[2] J.P. Mesirov, M.M. Sweet, Continued fraction expansions of rational expressions with irreducible denominators of characteristic 2, J. Number Theory 27 (1987) 144–148.
[3] H. Niederreiter, Dyadic fractions with small partial quotients, Monatsh. Math. 101 (1986) 309–315.

[4] H. Niederreiter, Rational functions with partial quotients of small degree in their continued fraction expansion, Monatsh. Math. 103 (1987) 269–288.
[5] O. Perron, Die Lehre von den Kettenbrüchen, Chelsea Publishing Company, New York, 1929.
[6] A.J. van der Poorten, An introduction to continued fractions, in: Diophantine Analysis, Cambridge Univ. Press, 1986, pp. 99–138.
[7] M. Yodphotong, V. Laohakosol, Proofs of Zaremba's Conjecture for powers of 6, in: Proc. Internat. Conf. Algebra Appl., 2002, pp. 278–282.